10/079,405
07/13/06

Reference 2

JP 2001-77857 A
[0003]

As a method of allowing the firewall 103 to realize such a security function, there is a method such as packet filtering. This packet filtering is performed as follows, for example. That is to say, as to a packet sent from the server 104 or the client 101, the firewall 103 determines whether to allow the packet to pass through, based on the IP address, the port number, etc, of the packet, the port number indicating the type of higher-ranked applications. A packet that is allowed to pass through is transferred to a counterpart as it is.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-077857
(43)Date of publication of application : 23.03.2001

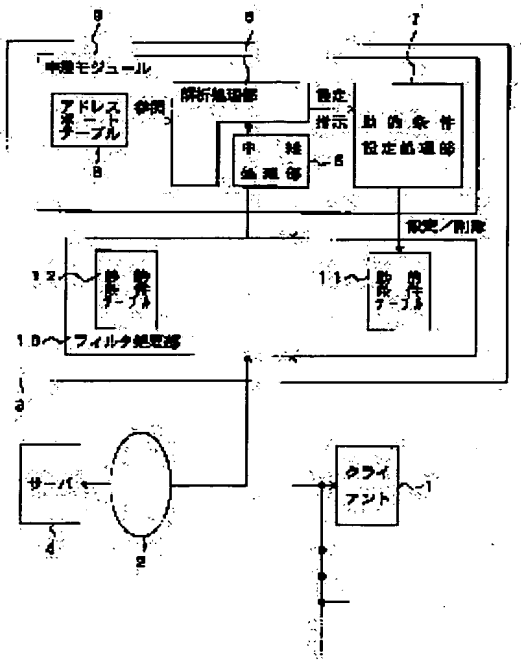
(51)Int.Cl. H04L 12/56
G06F 13/00
H04L 12/28
H04L 12/66

(21)Application number : 11-253871
(22)Date of filing : 08.09.1999

(71)Applicant : PFU LTD
(72)Inventor : YAMAMOTO MASAO

(54) FILTERING PROCESSING DEVICE, NETWORK PROVIDED WITH IT AND ITS STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To enhance the security of clients in a filtering processing device.
SOLUTION: The filtering processing device 3 is provided between a client 1 and a sever 4 to filter data sent/received between them. The filtering processing device 3 is provided with an analysis processing section 6 and a dynamic condition setting processing section 7. The analysis processing section 6 analyzes data sent from the client 1 to the server 4. The dynamic condition setting processing section 7 sets a filtering conditions as to data sent from the server 4 to the client 1 on the basis of the analysis result by the analysis processing section 6.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－77857
（P2001－77857A）
(43)公開日　平成13年３月23日(2001.3.23)

(51)Int.Cl.⁷		識別記号	Ｆ Ｉ		テーマコード（参考）	
Ｈ０４Ｌ	12/56		Ｈ０４Ｌ	11/20	１０２Ａ	５Ｂ０８９
Ｇ０６Ｆ	13/00	３５１	Ｃ０６Ｆ	13/00	３５１Ｚ	５Ｋ０３０
Ｈ０４Ｌ	12/28		Ｈ０４Ｌ	11/00	３１０Ｄ	５Ｋ０３３
	12/66			11/20	Ｂ	

審査請求　未請求　請求項の数12　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－253871

(22)出願日　平成11年９月８日(1999.9.8)

(71)出願人　000136136
株式会社ピーエフユー
石川県河北郡宇ノ気町字宇野気ヌ98番地の２

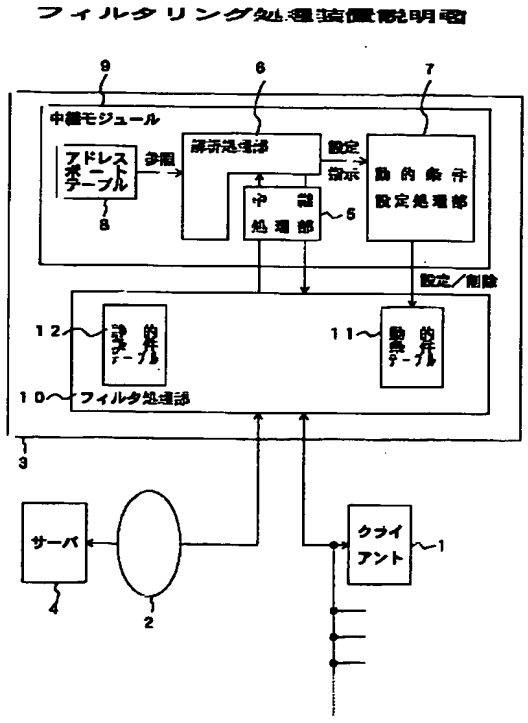
(72)発明者　山本　昌夫
石川県河北郡宇ノ気町字宇野気ヌ98番地の２　株式会社ピーエフユー内

(74)代理人　100074848
弁理士　森田　寛　（外１名）

最終頁に続く

(54)【発明の名称】　フィルタリング処理装置及びこれを備えるネットワーク及びその記憶媒体

(57)【要約】
【課題】　本発明は、フィルタリング処理装置に関し、クライアントのセキュリティを向上することを目的とする。
【解決手段】　フィルタリング処理装置３はクライアント１とサーバ４との間に設けられ、これらの間において送受信されるデータのフィルタリングを行う。フィルタリング処理装置３は解析処理部６と動的条件設定処理部７とを備える。解析処理部６はクライアント１からサーバ４に対して送信されるデータを解析する。動的条件設定処理部７は、解析処理部６における解析結果に基づいて、サーバ４からクライアント１に対して送信されるデータについてのフィルタリングの条件を設定する。



【特許請求の範囲】
【請求項１】　クライアントとサーバとの間に設けられ、これらの間において送受信されるデータのフィルタリングを行うフィルタリング処理装置であって、
前記クライアントから前記サーバに対して送信されるデータを解析する解析処理部と、
前記解析処理部における解析結果に基づいて、前記サーバから前記クライアントに対して送信されるデータについてのフィルタリングの条件を設定する動的条件設定処理部とを備えることを特徴とするフィルタリング処理装置。
【請求項２】　前記クライアントとサーバとの間において送受信されるデータはパケットからなることを特徴とする請求項１に記載のフィルタリング処理装置。
【請求項３】　当該フィルタリング処理装置が、更に、前記動的条件設定処理部により設定された条件に従って、当該フィルタリング処理装置を通過しようとするデータについてのフィルタリングを行うフィルタ処理部を備えることを特徴とする請求項１に記載のフィルタリング処理装置。
【請求項４】　前記解析処理部の解析するデータは、前記クライアントからの前記サーバに対する第１のコネクションを介して、前記クライアントから送信されるデータであり、
前記動的条件設定処理部の設定する条件は、前記第１のコネクションに対応する前記サーバからの前記クライアントに対する第２のコネクションを介して、前記サーバから送信されるデータについてのフィルタリングの条件であることを特徴とする請求項１に記載のフィルタリング処理装置。
【請求項５】　前記解析処理部の解析するデータは、前記サーバ及びクライアントの間における前記第２のコネクションについての制御情報を含むことを特徴とする請求項４に記載のフィルタリング処理装置。
【請求項６】　前記第２のコネクションについての制御情報は、前記第２のコネクションを開設するための制御情報であり、
前記第２のコネクションを開設するための制御情報に基づいて、前記動的条件設定処理部が前記フィルタリングの条件を設定することを特徴とする請求項５に記載のフィルタリング処理装置。
【請求項７】　前記第２のコネクションについての制御情報は、前記第２のコネクションを閉塞するための制御情報であり、
前記第２のコネクションを閉塞するための制御情報に基づいて、前記動的条件設定処理部が前記フィルタリングの条件を削除することを特徴とする請求項５に記載のフィルタリング処理装置。
【請求項８】　前記クライアントからの前記サーバに対する第１のコネクションが存在する場合に、
前記解析処理部が、前記クライアントから送信されるデータを解析し、
前記動的条件設定処理部が、前記解析結果に基づいて、前記第１のコネクションに対応する前記サーバからの前記クライアントに対する第２のコネクションにおいて前記サーバから送信されるデータについてのフィルタリングの条件を設定することを特徴とする請求項１に記載のフィルタリング処理装置。
【請求項９】　前記クライアントからの前記サーバに対する第２のコネクションが存在する場合に、
前記解析処理部が、前記クライアントから送信されるデータを解析し、
前記動的条件設定処理部が、前記解析結果に基づいて、前記第２のコネクションにおけるフィルタリングの条件を削除することを特徴とする請求項８に記載のフィルタリング処理装置。
【請求項１０】　前記解析処理部が、第２のコネクションにおけるフィルタリング以外のフィルタリングについての条件を備えることを特徴とする請求項１に記載のフィルタリング処理装置。
【請求項１１】　クライアントと、
サーバと、
前記クライアントとサーバとの間に設けられ、これらの間において送受信されるデータのフィルタリングを行うフィルタリング処理装置とを備え、
前記フィルタリング処理装置が、
前記クライアントから前記サーバに対して送信されるデータを解析する解析処理部と、
前記解析処理部における解析結果に基づいて、前記サーバから前記クライアントに対して送信されるデータについてのフィルタリングの条件を設定する動的条件設定処理部と、
前記動的条件設定処理部により設定された条件に従って、当該フィルタリング処理装置を通過しようとするデータについてのフィルタリングを行うフィルタ処理部を備えることを特徴とするネットワーク。
【請求項１２】　クライアントとサーバとの間において送受信されるデータのフィルタリングを行うプログラムを格納したコンピュータ読取可能な記憶媒体において、当該プログラムは、
前記クライアントから前記サーバに対して送信されるデータを解析する第１のプログラムコードと、
前記解析結果に基づいて、前記サーバから前記クライアントに対して送信されるデータについてのフィルタリングの条件を設定する第２のプログラムコードとを有することを特徴とするコンピュータ読取可能な記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、フィルタリング処理装置及びこれを備えるネットワーク及びその記憶媒体

に関し、特に、クライアントのセキュリティを向上したフィルタリング処理装置及びこれを備えるネットワーク及びその記憶媒体に関する。

【０００２】

【従来の技術】インターネットにおいては、クライアント（ＷＷＷブラウザ）に対して、種々のサーバが接続してくる。そこで、セキュリティの確保のために、図７（Ａ）に示すように、インターネット１０２とクライアント１０１との間にファイアウォール１０３が設けられる。クライアント１０１又はサーバ１０４から送出されたパケットは、ファイアウォール１０３を通過することが認められれば、これを越えて通信の相手方に到達することができる。

【０００３】ファイアウォール１０３がこのようなセキュリティ機能を実現する方法には、例えばパケットフィルタリング等の方法がある。このパケットフィルタリングは、例えば、以下のように行われる。即ち、サーバ１０４又はクライアント１０１から送られたパケットについて、ファイアウォール１０３が、パケットのＩＰアドレスや上位アプリケーションの種類を示すポート番号等に基づいて、当該パケットを通過させるか否かを決定する。通過させると決定されたパケットは、そのまま相手方に転送される。

【０００４】

【発明が解決しようとする課題】大量のデータ転送を頻繁に行うようなネットワークでは、通信経済の観点から、通常、クライアント１０１とサーバ１０４との間の通信は、以下のように行われる。即ち、クライアント１０１からサーバ１０４への接続（以下、第１のコネクションと言う）を確立し、この第１のコネクションによりクライアント１０１からサーバ１０４へ要求を通知するための制御用の通信を行う。次に、第１のコネクションとは別に、サーバ１０４からクライアント１０１への接続（以下、第２のコネクションと言う）を確立し、この第２のコネクションによりデータ送信用の通信を行う。第２のコネクションにおいては、一般に、既に接続済の通信路を使用した通信の待ち合わせ又は受信ポートの指定が可能である。

【０００５】そこで、ファイアウォール１０３を採用するネットワークにおいて、上記第２のコネクションを許す場合、ファイアウォール１０３に、当該第２のコネクションにおけるパケットについてのパケットフィルタリング（通過）の条件を、予め設定しておく必要がある。

【０００６】このような第２のコネクションについてのパケットフィルタリングの一例として、例えばＦＴＰ（ファイルトランスファープロトコル）の場合について説明する。ＦＴＰにおいては、データ転送時にサーバ１０４の固定ポート（ポート番号２０）からクライアント１０１のＡＮＹポートに接続する（コネクションを確立する）。ここで、ＡＮＹポートは、サーバ１０４がクライアント１０１からの通知に基づいて当該通信毎に割り当てるポートであり、そのポート番号は予め１０２４～６５５３５の範囲とされる。従って、第２のコネクションについてのパケットフィルタリングの条件テーブル１１１は、図７（Ｂ）に示すように、送信先のポート番号が１０２４～６５５３５であるパケットについて通過させる設定とされる。即ち、ファイアウォール１０３は、サーバＩＰアドレスＳのポート番号２０からのクライアントＩＰアドレスＣへのパケットについては、送信先のポート番号が１０２４～６５５３５の範囲であれば、通過させることになる。

【０００７】このため、第２のコネクションにおいては、クライアント１０１から見ると、サーバＩＰアドレスＳのポート番号２０からのパケットであれば、ポート番号が１０２４～６５５３５と言う広範囲のものがファイアウォール１０３を通過する。従って、極めて広範囲のパケットについて、ファイアウォール１０３が存在しないように見えることになる。即ち、ファイアウォール１０３の内側に保護されているはずのクライアント１０１が、極めて広範囲のパケットについて無防備な状態に置かれていることになる。

【０００８】本発明は、クライアントのセキュリティを向上したフィルタリング処理装置を提供することを目的とする。

【０００９】また、本発明は、クライアントのセキュリティを向上したネットワークを提供することを目的とする。

【００１０】また、本発明は、クライアントのセキュリティを向上したフィルタリング処理装置を実現するプログラムを記憶する記憶媒体を提供することを目的とする。

【００１１】

【課題を解決するための手段】図１は本発明の原理構成図であり、本発明によるフィルタリング処理装置３を示す。フィルタリング処理装置３はクライアント１とサーバ４との間に設けられ、これらの間において送受信されるデータのフィルタリングを行う。フィルタリング処理装置３は解析処理部６と動的条件設定処理部７とを備える。解析処理部６はクライアント１からサーバ４に対して送信されるデータを解析する。動的条件設定処理部７は、解析処理部６における解析結果に基づいて、サーバ４からクライアント１に対して送信されるデータについてのフィルタリングの条件を設定する。

【００１２】本発明のフィルタリング処理装置３によれば、クライアント１からサーバ４に対して送信されるデータの解析結果に基づいて、サーバ４からクライアント１に対して送信されるデータについてのフィルタリングの条件を動的に設定することができる。従って、当該条件を満たすデータのみがフィルタリング処理装置３を通過するように設定することができる。例えば、前述のよ

うに第２のコネクションを許す場合、クライアント１からサーバ４へのデータから、クライアント１におけるデータの送受信の条件を検出する。これにより、第２のコネクションにおいてサーバ４からクライアント１へのデータがどのような条件で送信されるかを予め知り、これに基づいて、サーバ４からクライアント１へのデータの内で当該送信の条件に合致するデータのみが、第２のコネクションにおいてフィルタリング処理装置３を通過するように設定することができる。従って、第２のコネクションにおいて、クライアント１から見て、同一のサーバ４からのデータであっても、フィルタリングの条件を満たさないデータはフィルタリング処理装置３を通過することができない。これにより、クライアント１をフィルタリング処理装置３の内側に保護することができ、そのセキュリティを向上することができる。

【００１３】

【発明の実施の形態】図２はフィルタリング処理装置説明図であり、本発明のフィルタリング処理装置３及びこれを備えるネットワークの構成を示す。

【００１４】図２において、フィルタリング処理装置３は、例えばファイアウォール３からなる。ファイアウォール３は、クライアント１のセキュリティの確保のために、ネットワーク２とクライアント１との間に設けられ、フィルタリングを行う。従って、サーバ４から見た場合、クライアント１はファイアウォール３の内側にあり、これにより守られている。例えば、（複数の）クライアント１はファイアウォール３と共にイントラネットを構成する。ネットワーク２は、例えばインターネット２からなる。サーバ４はウェブ（Ｗｅｂ）サーバやプロキシサーバ等からなる。従って、全体をネットワークとして見ると、クライアント１、サーバ４、ファイアウォール３とを備える。

【００１５】クライアント１は、例えば、インターネット２を介して、サーバ４にアクセスする。この時、クライアント１は、ファイアウォール３にアクセスしてそのフィルタ処理部１０を通過する必要がある。逆に、クライアント１に応答するサーバ４も、ファイアウォール３にアクセスしてそのフィルタ処理部１０を通過する必要がある。従って、ファイアウォール３は、その内側のクライアント１（の属するイントラネット）と外側のインターネット２とを切り離す。フィルタ処理部１０を通過すれば、クライアント１とサーバ４とはファイアウォール３を越えて相互にアクセスすることができる。

【００１６】ファイアウォール３は、中央演算処理装置（ＣＰＵ）、主メモリ、補助記憶等（いずれも図示せず）からなる。主メモリ上に、フィルタリング処理を行うプログラムが存在する。フィルタリング処理プログラムがＣＰＵ上で実行されることにより、以下に説明する各処理部５、６、７、１０によるフィルタリング処理が行われる。なお、アドレスポートテーブル８、動的条件テーブル１１、静的条件テーブル１２は磁気ディスク装置等の補助記憶に設けられる。

【００１７】ファイアウォール３は、前述のように、クライアント１のセキュリティの実現のために、クライアント１とサーバ４との間に設けられ、これらの間において送受信されるデータのフィルタリング処理を行う。クライアント１とサーバ４との間において送受信されるデータはパケットからなる。従って、ファイアウォール３はパケットフィルタリングによりクライアント１のセキュリティを実現する。このために、ファイアウォール３は、中継モジュール９、フィルタ処理部１０を備える。中継モジュール９は、フィルタ処理部１０を制御し、また、そのための制御情報（フィルタリングの制御のための情報）を作成する。フィルタ処理部１０は、中継モジュール９の制御に従って、クライアント１又はサーバ４から受信したパケットについてのフィルタリングを行う。中継モジュール９は、中継処理部５、解析処理部６、動的条件設定処理部７を備える。

【００１８】フィルタ処理部１０は、動的条件設定処理部７により設定された条件に従って、当該ファイアウォール３を通過しようとするデータについての実際のフィルタリング処理及び通信処理を行う。即ち、フィルタ処理部１０は、クライアント１又はサーバ４から送信されてきたパケットの受信処理を行い、フィルタリングの制御のための情報（動的フィルタリング情報）を抽出するために、これを中継モジュール９に送る。また、フィルタ処理部１０は、中継モジュール９からのパケットを受け取り、予め自己が備えるフィルタリングの制御のための情報（静的フィルタリング情報）と中継モジュール９から与えられたフィルタリングの制御のための情報（動的フィルタリング情報）とに従ってフィルタリングした後、通過させるべきパケットの当該クライアント１又はサーバ４への送信処理を行う。

【００１９】このために、フィルタ処理部１０は、図３（Ｂ）に示すように、動的条件テーブル１１を備える。動的条件テーブル１１は、中継モジュール９からのフィルタリングの制御のための情報（動的フィルタリング情報）を格納する。動的フィルタリング情報は、第２のコネクションにおけるフィルタリングについての条件を規定する情報である。動的フィルタリング情報は、後述するように、動的条件設定処理部７により設定され、削除される。

【００２０】フィルタ処理部１０は、動的条件テーブル１１とは別に、第２のコネクションにおけるフィルタリング以外のフィルタリング（例えば、第１のコネクションにおけるフィルタリング）についての条件（静的フィルタリング情報）を備える。このために、フィルタ処理部１０は、図３（Ａ）に示すように、静的条件テーブル１２を備える。静的条件テーブル１２は、静的フィルタリング情報を格納する。静的フィルタリング情報は、第

１のコネクションにおけるフィルタリングについての条件を規定する情報である。

【００２１】図３（Ａ）に示す静的条件テーブル１２は、例えばＦＴＰの場合について示す。ＦＴＰにおいては、処理「通過」の対象として、送信元アドレスとしてクライアント１の「クライアントＩＰアドレスＣ」、そのポート（送信元ポート）番号として「１０２４～６５５３５」、送信先アドレスとしてサーバ４の「サーバＩＰアドレスＳ」、そのポート（送信先ポート）番号として「２１」が設定される。クライアント１の送信ポート番号が「１０２４～６５５３５」のように広範囲であるが、ファイアウォール３の内側であるので、セキュリティ上の問題はない。サーバ４の受信ポート番号「２１」は固定である。従って、第１のコネクションについてのパケットフィルタリング（静的フィルタリング）は、クライアントＩＰアドレスＣのポート番号１０２４～６５５３５からのサーバＩＰアドレスＳのポート番号２１へのパケットについては、通過させることになる。

【００２２】また、このようなパケットに対する第１のコネクション上の応答パケットについても、通過させることになる。例えば、クライアント１からのパケットの送信ポートが１０２４であるとすると、サーバＩＰアドレスＳのポート番号２１からのクライアントＩＰアドレスＣのポート番号１０２４へのパケットについても、通過させることになる。これは、一旦確立された第１のコネクションに接続する特定のサーバ４及びクライアント１の間での通信であり、かつ、一旦静的フィルタリングを通過した送受信のポートの間での通信だからである。即ち、同一のクライアント１及びサーバ４の間の同一のポートでの通信だからである。

【００２３】このために、フィルタ処理部１０は、図３（Ａ）に示す静的条件テーブル１２において、処理「通過」の対象として、送信元アドレスとしてサーバ４の「サーバＩＰアドレスＳ」、そのポート（送信元ポート）番号として「２１」、送信先アドレスとしてクライアント１の「クライアントＩＰアドレスＣ」、そのポート（送信先ポート）番号として「１０２４」を設定する。このフィルタリングの条件は、図３（Ａ）に示す条件の裏返しの条件である。

【００２４】中継モジュール９において、中継処理部５はデータの中継を行う。即ち、中継処理部５は、フィルタ処理部１０からパケットを受け取り、動的フィルタリング情報を抽出するために、これを解析処理部６へ送る。また、中継処理部５は、解析処理部６からパケットを受け取り、フィルタリングのために、これをフィルタ処理部１０に送る。

【００２５】解析処理部６は、クライアント１からサーバ４に対して送信されるデータを解析する。具体的には、解析処理部６の解析するデータは、クライアント１からサーバ４に対して確立されたコネクション（第１のコネクション）を介して、クライアント１から送信されるデータである。このデータは、第１のコネクションとは別に、サーバ４からクライアント１に対してその時点以後に確立される（又はその時点前に確立された）コネクション（第２のコネクション）についての情報を含む。第２のコネクションについての情報は、第２のコネクションを開設するための情報、又は、第２のコネクションを閉塞するための情報である。

【００２６】この明細書において、第１及び第２のコネクションは、トランスポート層でのＴＣＰ（トランスミッションコントロールプロトコル）の接続である。第２のコネクションは、第１のコネクションが確立された後にそれが存在する状態で確立され、クライアント１からサーバ４へのコネクションである第１のコネクションとは逆に、サーバ４からクライアント１へのコネクションである。従って、第２のコネクションは、第１のコネクションの存在が前提であって、前提である当該第１のコネクションに対応する。

【００２７】前述のように、パケットフィルタリングにおいては、パケットのＩＰアドレスや上位アプリケーションの種類を示すポート番号等に基づいて、当該パケットを通過させるか否かを決定する。従って、解析処理部６は、第２のコネクションを使用するネットワークアプリケーションのプロトコルデータを解析し、ＩＰアドレスやポート番号等の接続に関する情報を、第２のコネクションについての情報として取得する。

【００２８】例えば、ＦＴＰにおいては、第１のコネクションを介して、第２のコネクションについての情報が、所定のコマンドによりクライアント１からサーバ４に通知される。具体的には、クライアント１からのポート（ＰＯＲＴ）コマンド及びこれに続くデータ受信コマンドにより、当該第１のコネクションを介しての通信の後、サーバ４からクライアント１への第２のコネクションが確立される。データ受信コマンドとしてはＬＩＳＴ、ＲＥＴＲ又はＳＴＯＲ等がある。また、当該ポートコマンドにより、第２のコネクションの利用時にクライアント１においてデータを受信するポートのアドレス及び当該ポートについての情報が、クライアント１からサーバ４に通知される。この情報は、(ASCII) 文字列として通知され、例えば、ポートアドレス「192.168.1.1.4.1 」と、ＩＰアドレス「192.168.1.1」とポート番号「1025」とからなる（図３（Ｂ）参照）。

【００２９】従って、解析処理部６は、第１のコネクション上のクライアント１からのパケットを解析し、ポートコマンドに続くデータ受信コマンドを検出すると、ポートコマンドにおける前記３個のデータを第２のコネクションについてのそれを開設させるための情報として抽出する。従って、第２のコネクションを用いた通信のフィルタリングにおいては、当該ＩＰアドレスのクライアント１の当該ポート（及びアドレス）に対して当該サー

バ４から送信されるパケットのみを通過させれば良い。

【００３０】また、クライアント１からのポートコマンド及びこれに続くデータ受信完了コマンドにより、当該第１のコネクションを介しての通信の後、第２のコネクションが閉塞される。従って、解析処理部６は、第１のコネクション上のクライアント１からのパケットを解析し、ポートコマンドに続くデータ受信完了コマンドを検出すると、前記と同様にポートコマンドにおける前記３個のデータを第２のコネクションについてのそれを閉塞させるための情報として抽出する。

【００３１】なお、実際は、第１のコネクションに対して既に第２のコネクションが開設された状態で、更に、ポートコマンド及びこれに続くデータ受信コマンドが検出されると、当該既設の第２のコネクションは閉塞され、これとは別に新たな第２のコネクションが開設される。従って、既設の第２のコネクションについての動的フィルタリング条件は削除され、新たな第２のコネクションについての動的フィルタリング条件が設定される。

【００３２】解析処理部６は、第２のコネクションにおけるフィルタリングについての条件（動的フィルタリング情報）を作成するために、アドレスポートテーブル８を備える。アドレスポートテーブル８は、アドレスポート情報を格納する。アドレスポート情報は、第２のコネクションが対応する第１のコネクションのサーバ４のサーバＩＰアドレスとそのデータ送信ポートとからなる。

【００３３】例えば、ＦＴＰにおいては、サーバ４におけるデータの送信ポートは、第１のコネクションのサーバＩＰアドレス「192.168.1.1 」と固定ポート２０番とに固定されている。これらが、サーバ４についてのアドレスポート情報として、当該アドレスポートテーブル８に格納される。

【００３４】従って、ＦＴＰにおいては、解析処理部６により、図３（Ｂ）に示すように、動的フィルタリング情報が作成される。即ち、前述の３個のデータの内、ポートアドレス「192.168.1.1.4.1 」を用いてサーバ４のサーバＩＰアドレスを求め、また、当該ポートアドレスを用いてアドレスポートテーブル８を参照し、当該アドレスのサーバ４のデータ送信（送信元）ポート（ポート番号２０）を求める。このポート番号２０は、前述のように、固定である。また、３個のデータの内、ＩＰアドレス「192.168.1.1 」をクライアント１のクライアントＩＰアドレスとし、ポート番号「１０２５」をクライアント１のデータ受信（送信先）ポートとする。これにより、第２のコネクションにおいて、サーバ４から送信されるパケットは、送信先ポートが１０２５であるもののみがフィルタリングを通過できることになる。

【００３５】動的条件設定処理部７は、解析処理部６における解析結果に基づいて、サーバ４からクライアント１に対して送信されるデータについてのフィルタリングの条件（動的フィルタリング情報）を設定する。具体的には、動的条件設定処理部７の設定する条件は、第１のコネクションに対応するサーバ４からのクライアント１に対する第２のコネクションを介して、サーバ４から送信されるデータについての動的フィルタリングの条件である。従って、動的条件設定処理部７は、第２のコネクションを開設するための情報に基づいて動的フィルタリングの条件を設定し、又は、第２のコネクションを閉塞するための情報に基づいて動的フィルタリングの条件を削除する。

【００３６】クライアント１からのサーバ４に対する第１のコネクションが存在する場合に、第２のコネクションについての動的フィルタリングの条件が設定される。具体的には、第２のコネクションの使用（又は設定）の直前に、その直前に行われた第１のコネクションを使用した通信を解析した結果に基づいて設定される。即ち、動的に設定される。このために、解析処理部６が、クライアント１から送信されるデータを解析し、動的条件設定処理部７が、この解析結果に基づいて、第１のコネクションに対応するサーバ４からのクライアント１に対する第２のコネクションにおいて、サーバ４から送信されるデータについてのフィルタリングの条件を動的に設定する。従って、第２のコネクションにおけるフィルタリングの条件を、必要な場合にのみ、その直前に動的に設定し、フィルタリングを行うことができる。

【００３７】また、クライアント１からのサーバ４に対する第２のコネクションが存在する場合に、動的フィルタリングの条件が削除される。具体的には、第２のコネクションの使用（又は切断）の直後に、その直後に行われた第１のコネクションを使用した通信を解析した結果に基づいて、削除される。即ち、動的に削除される。このために、解析処理部６が、クライアント１から送信されるデータを解析し、動的条件設定処理部７が、解析結果に基づいて、第２のコネクションにおける動的フィルタリングの条件を削除する。従って、第２のコネクションにおけるフィルタリングの条件を、その直後に動的に削除することができる。

【００３８】なお、実際は、第２のコネクションが対応する第１のコネクションが切断される場合、当該第２のコネクションも切断（閉塞）される。従って、この場合にも、その動的フィルタリングの条件が削除される。具体的には、クライアント１からサーバ４に対して第１のコネクションの切断が通知されたら、これを解析処理部６が検出して、動的条件設定処理部７により当該第２のコネクションが閉塞される。

【００３９】例えば、前述のＦＴＰにおいては、動的条件設定処理部７は、解析処理部６により図３（Ｂ）に示すように作成された動的フィルタリング情報を当該情報の設定指示と共に受け取り、当該情報をフィルタ処理部１０の動的条件テーブル１１に書き込む。これにより、フィルタ処理部１０における動的フィルタリングの条件

が設定される。この結果、第２のコネクションにおいて、サーバ４から送信されるパケットは、送信先ポートが１０２５であるもののみがフィルタリングを通過できることになる。

【００４０】図４は、ファイアウォール３が実行するフィルタリング処理フローを示す。

【００４１】フィルタ処理部１０が、パケットを受信したか否かを調べる（ステップＳ１）。受信していない場合、ステップＳ１を繰り返す。

【００４２】受信した場合、フィルタ処理部１０が、静的条件テーブル１２及び動的条件テーブル１１を用いて、静的フィルタリング処理及び動的フィルタリング処理を行う（ステップＳ２）。この時、フィルタ処理部１０は、当該パケットが第１又は第２のコネクション上のものか及びクライアント１又はサーバ４からのものかを意識することはなく、また、静的フィルタリングか動的フィルタリングかを意識することはない。

【００４３】フィルタ処理部１０が、フィルタリング処理の結果、当該パケットが通過の条件を満足するか否かを調べる（ステップＳ３）。

【００４４】満足する場合、フィルタ処理部１０が、当該パケットを中継モジュール９に送る（ステップＳ４）。当該パケットは、中継モジュール９において、中継処理部５を介して、解析処理部６に送られる。

【００４５】解析処理部６が、当該パケットを解析する（ステップＳ５）。

【００４６】この解析の結果に基づいて、所定の処理が行われる（ステップＳ６）。これについては、図５を参照して後述する。

【００４７】解析処理部６が、当該パケットをフィルタ処理部１０に送る（ステップＳ７）。

【００４８】フィルタ処理部１０が、当該パケットを中継処理する（ステップＳ８）。即ち、当該パケットをその宛て先（送信先）に転送する。

【００４９】ステップＳ３において通過の条件を満足しない場合、フィルタ処理部１０が、当該パケットを廃棄する（ステップＳ９）。

【００５０】図５は、図４のステップＳ６においてファイアウォール３が実行するフィルタリング条件設定処理フローを示す。

【００５１】解析処理部６が、中継処理部５から受け取ったパケットについて解析する（ステップＳ１１）。

【００５２】解析処理部６が、当該解析結果に基づいて、第２のコネクションの開設についての情報か否かを調べる（ステップＳ１２）。当該情報でない場合、ステップＳ１５に進む。なお、このパケットは、フィルタ処理部１０がクライアント１から受け取って中継処理部５に渡し、更に、中継処理部５が解析処理部６に渡したものである。

【００５３】当該情報である場合、解析処理部６が、当該解析結果に基づいて、第２のコネクションにおけるパケットフィルタリングの条件を作成し、動的条件設定処理部７に条件の設定を依頼する（ステップＳ１３）。

【００５４】依頼を受けた動的条件設定処理部７が当該条件をフィルタ処理部１０に設定する（ステップＳ１４）。この後、中継処理部５がパケットの中継処理を行う（図４のステップＳ７及びＳ８）。即ち、解析処理部６が、必要に応じてパケットのデータを書き替えた上で、当該パケットをフィルタ処理部１０に返し、フィルタ処理部１０が当該パケットをサーバ４に送信する。

【００５５】ステップＳ１２において第２のコネクションの開設についての情報でない場合、更に、解析処理部６が、第２のコネクションの閉塞についての情報か否かを調べる（ステップＳ１５）。当該情報でない場合、図４のステップＳ７に進む。

【００５６】当該情報である場合、解析処理部６が、当該解析結果に基づいて、第２のコネクションにおけるパケットフィルタリングの条件の削除を、動的条件設定処理部７に依頼し、依頼を受けた動的条件設定処理部７が、当該条件をフィルタ処理部１０から削除する（ステップＳ１６）。

【００５７】図６は、クライアント１とサーバ４との間における通信について、ファイアウォール３が実行するフィルタリング処理説明図を示す。

【００５８】クライアント１からファイアウォール３を介してサーバ４に対するコネクション（第１のコネクション）を張る（①）。

【００５９】クライアント１が、第１のコネクション上でサーバ４に対する制御用のパケットを送信すると、ファイアウォール３が図３（Ａ）に示す静的フィルタリング条件によりフィルタリングを行い（②のａ）、当該パケットを通過させるか否かを判断し、条件を満たすパケットであればサーバ４に転送する（②）。この時、当該パケットがクライアント１からのものであるので、解析処理部６が当該パケットを解析する。この結果、第２のコネクションを開設するための情報が抽出されないので、動的条件設定処理部７による動的フィルタリング条件の設定は行われない。

【００６０】パケットを受信したサーバ４が、クライアント１に対する応答のパケットを送信すると、ファイアウォール３が図３（Ａ）に示す静的フィルタリング条件の裏返しの条件によりフィルタリングを行い（③のａ）、当該パケットを通過させるか否かを判断し、条件を満たすパケットであればクライアント１に転送する（③）。

【００６１】クライアント１がサーバ４に対するデータ転送要求（制御用）のパケットを送信すると、ファイアウォール３が図３（Ａ）に示す静的フィルタリング条件によりフィルタリングを行い（④のａ）、当該パケットを通過させるか否かを判断し、条件を満たすパケットで

あればサーバ４に転送する（㊹）。この時、当該パケットがクライアント１からのものであるので、解析処理部６が当該パケットを解析する。この結果、第２のコネクションを開設するための情報が抽出されるので、動的条件設定処理部７により、フィルタ処理部１０の動的条件テーブル１１への図３（Ｂ）に示す動的フィルタリング条件の設定が行われる。

【００６２】パケットを受信したサーバ４が、第１のコネクションとは別に、当該サーバ４からファイアウォール３を介してクライアント１に対するコネクション（第２のコネクション）を張る（㊺）。

【００６３】サーバ４が、クライアント１に対する転送データのパケットを送信すると、ファイアウォール３が図３（Ｂ）に示す動的フィルタリング条件によりフィルタリングを行い（㊻のｂ）、当該パケットを通過させるか否かを判断し、条件を満たすパケットであればクライアント１に転送する（㊼）。

【００６４】データを受信したクライアント１は、サーバ４に対するデータ受信完了通知（制御用）のパケットを送信すると、ファイアウォール３が図３（Ａ）に示す静的フィルタリング条件によりフィルタリングを行い（㊽のａ）、当該パケットを通過させるか否かを判断し、条件を満たすパケットであればサーバ４に転送する（㊾）。この時、当該パケットがクライアント１からのものであるので、解析処理部６が当該パケットを解析する。この結果、第２のコネクションを閉塞するための情報が抽出されるので、動的条件設定処理部７により、フィルタ処理部１０の動的条件テーブル１１からの図３（Ｂ）に示す動的フィルタリング条件の削除が行われる。

【００６５】サーバ４が、当該サーバ４からクライアント１に対するコネクション（第２のコネクション）を切断する（㊿）。

【００６６】以上、本発明をその実施の態様により説明したが、本発明はその主旨の範囲において種々の変形が可能である。

【００６７】例えば、動的フィルタリング条件の作成は、解析処理部６ではなく、動的条件設定処理部７又はフィルタ処理部１０が行ってもよい。また、解析処理部６と動的条件設定処理部７とを一体に設けてもよい。

【００６８】また、本発明は、ＦＴＰに限らず、例えばｔｅｌｎｅｔ等の種々の通信プロトコルに適用することができる。例えば、ｔｅｌｎｅｔにおいては、フィルタ処理部１０における静的フィルタリングの後、そのまま中継処理を行うのではなく、当該パケットを中継モジュール９に送るようにすればよい。

【００６９】

【発明の効果】以上説明したように、本発明によれば、フィルタリング処理装置において、第１のコネクションにおいてクライアントからサーバに対して送信されるデータの解析結果に基づいて、第２のコネクションにおいてサーバからクライアントに対して送信されるデータについてのフィルタリングの条件を動的に設定することにより、第２のコネクションにおいてサーバからクライアントへのデータがどのような条件で送信されるかを予め知ることができるので、当該送信の条件に合致するサーバからクライアントへのデータのみがフィルタリング処理装置を通過するように設定することができ、結果として、第２のコネクションにおいて通過条件を満たさないデータをフィルタリング処理により除去することができ、クライアントをフィルタリング処理装置の内側に保護してそのセキュリティを向上することができる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】フィルタリング処理装置説明図である。

【図３】フィルタリング条件説明図である。

【図４】フィルタリング処理フローチャートである。

【図５】フィルタリング条件設定処理フローチャートである。

【図６】フィルタリング処理説明図である。

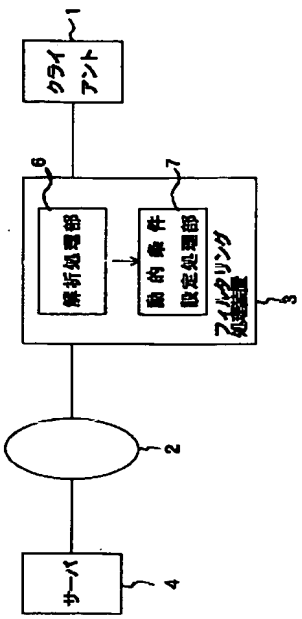
【図７】従来技術説明図である。

【符号の説明】

１　クライアント
２　インターネット
３　ファイアウォール
４　サーバ
５　中継処理部
６　解析処理部
７　動的条件設定処理部
８　アドレスポートテーブル
９　中継モジュール
１０　フィルタ処理部
１１　動的条件テーブル
１２　静的条件テーブル

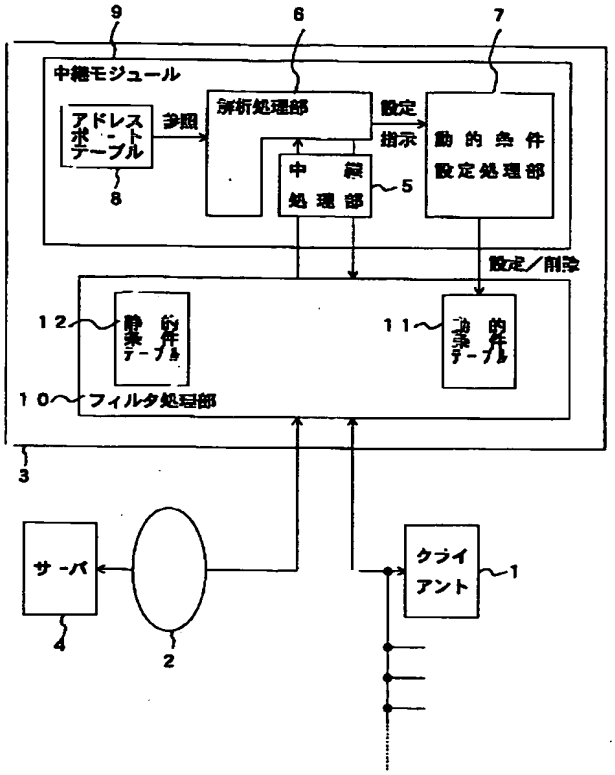
【図1】

本発明の原理構成図



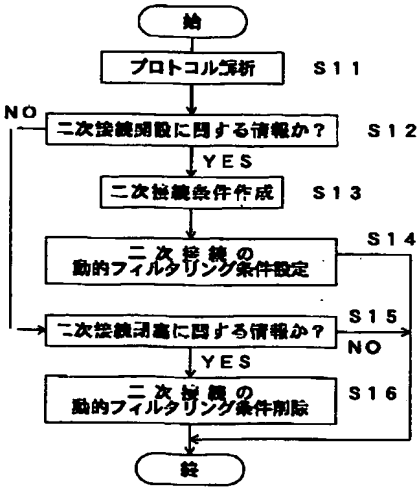
【図2】

フィルタリング処理装置説明図



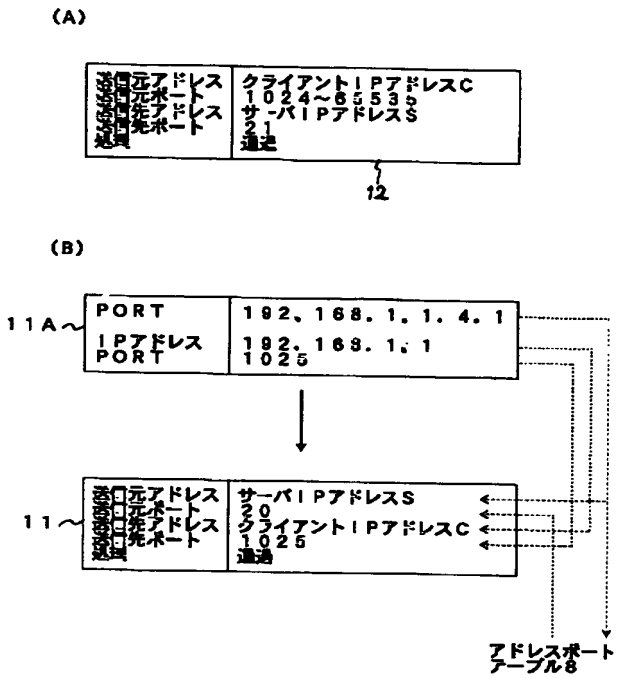
【図5】

フィルタリング条件設定処理フローチャート



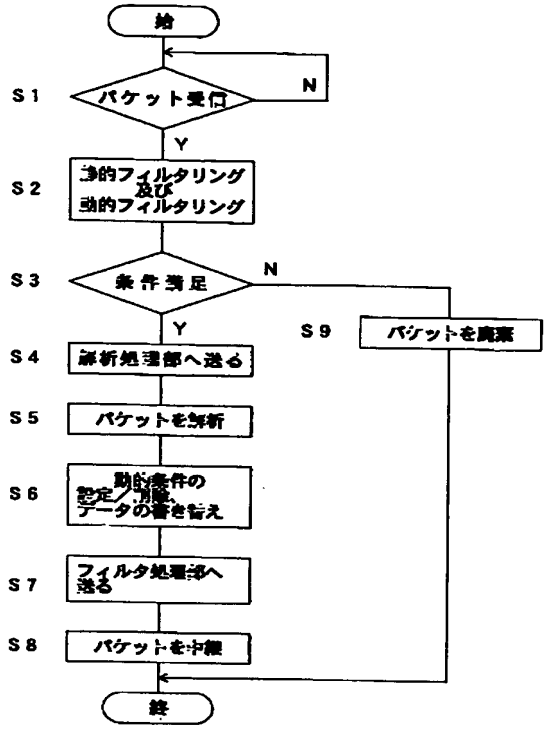
【図3】

フィルタリング条件説明図



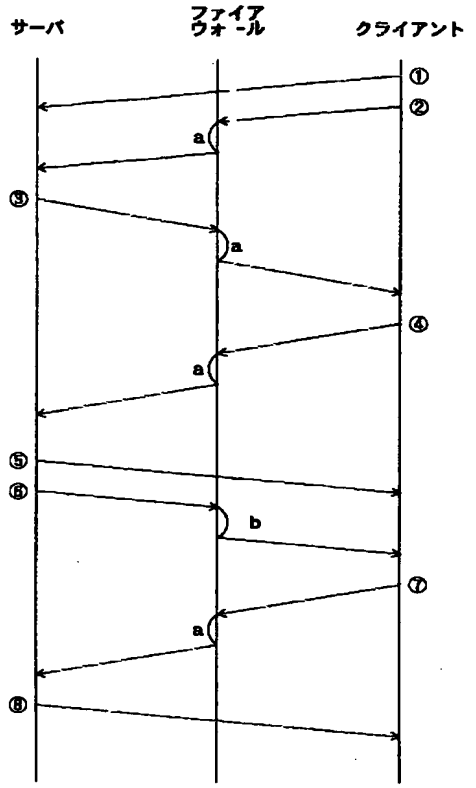
【図4】

フィルタリング処理フローチャート



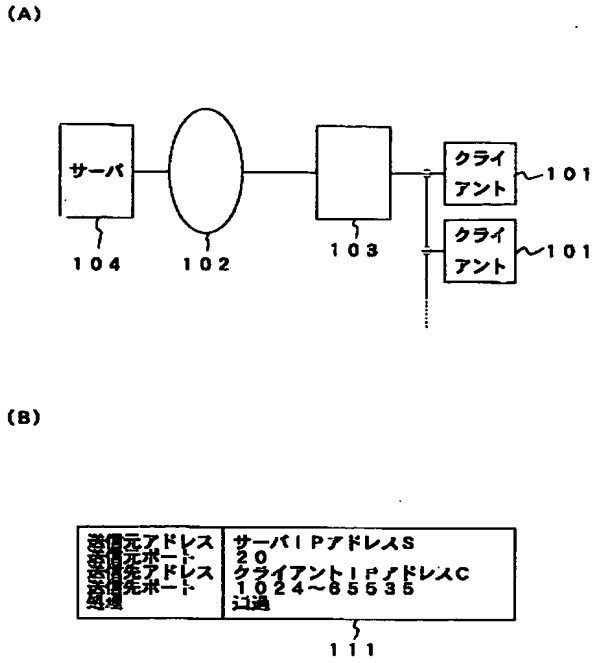
【図6】

フィルタリング処理説明図



【図7】

従来技術説明図



フロントページの続き

Fターム(参考) 5B089 GA11 GA21 HA10 HB04 JA40
KA17 KB13 KC52 KC58
5K030 GA15 HC01 HC14 HD03 HD06
KA07 LA01 LC15 LD20 LE17
MA04 MB00
5K033 AA01 AA03 CB03 CB06 CB08
DA05 DB12 DB14 DB16 DB18
DB20

Reference 3

JP 2000-32052 A

[0045] (A) In a case where a bandwidth reservation request arrives from a bandwidth reservation protocol of another router under such a condition that all bandwidths of routes between routers are used for transmitting packets, the router negotiates with an adjacent router, if the adjacent router is one according to this invention, to request use of one of sub-routes between them for the bandwidth reservation. If the adjacent router is a conventional one, the router performs a process according to a general RSVP.
[0046] (B) If a sub-route for the bandwidth reservation is set between the routers as a result of the negotiation, the router changes a routing table. In a general case of RSVP, the routing table contains destination IP address (network address), source IP address, destination port number, source port number, IP address of next router, and interface for next router (packet transfer means in this specification).
[0047] In this embodiment, as sub-route to a next router, there are plural routes, not one route. Therefore, the routing table specifies a plurality of output side packet transfer means. At the time of bandwidth reservation, the routing table is changed so as to specify an output side packet transfer means connected to a corresponding sub-route for a packet flow (one of entries of routing table) that needs bandwidth reservation.
[0048] (C) In a case where the bandwidth reservation can be made as a result of the negotiation (in a case where a sub-route for bandwidth reservation cannot be set between the routers), the transmission side transmits the packet by using an output-side packet transfer means for the sub-route set for the bandwidth reservation, and the receiving side receives the signal by using an input-side packet transfer means corresponding to the reserved sub-route.
(D) The reserved bandwidth becomes free because of a bandwidth release process by the bandwidth reservation protocol or time-out, and then all bandwidths between the routers can be used as usual.
[0049]

Next, an example of an operation flow in a case of using a method for unexplicitly performing bandwidth reservation will be described. In general, a bandwidth reservation protocol informs the router of a bandwidth reservation request, an above-described operation to keep a sub-route is performed for the bandwidth reservation in response to the request. By applying the same operation to high-priority packets, high throughput can be realized in an entire network.